Aruba WLAN 관리자를 위해 Umbrella DNS 구축

목차

소개

이 문서에서는 Aruba WLAN 관리자를 위해 Umbrella DNS 서비스를 구축하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 Cisco Umbrella를 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

개요

Aruba Networks는 각기 다른 시장 부문 및 구축 시나리오에 따라 다음과 같은 세 가지 무선 LAN(WLAN) 제품 라인 및 운영 체제를 갖추고 있습니다.

- ArubaOS: 대규모 조직 및 고밀도 구축
- Aruba Instant/InstantOS: SMB(중소, 중견, 성장 기업) 및 분산된 기업
- Aruba 인스턴트 켜짐: 가정 및 소규모 사무실 사용자용

이 문서에서는 Aruba WLAN 관리자가 Umbrella DNS 서비스를 채택하고 구축하기 위한 지침을 제공합니다.

구축 방법

구축 방법은 Aruba 운영 체제 및 Umbrella 사용 계획에 따라 다릅니다.

앞서 언급한 세 가지 Aruba 운영 체제 중 하나를 실행하는 경우 Umbrella 사용 설명서를 참조하여 Umbrella DNS 구축을 시작할 수 있습니다. 비디오 자습서도 제공됩니다.

Aruba Instant를 실행할 경우 InstantOS에서 사용할 수 있는 Umbrella 네트워크 디바이스 통합을 사용할 수 있는 추가 옵션이 있습니다. 그러나 이 옵션을 선택하면 Umbrella 보고에서 Activity Search 보고서와 같은 WLAN에 대한 무선 클라이언트의 내부/개인 IP 주소를 볼 수 없습니다. 클라이언트의 DNS 쿼리는 Umbrella에서 Instant AP 클러스터의 네트워크 디바이스 ID에 매핑되며 개별 클라이언트에 대한 정보를 사용할 수 없습니다. Umbrella 클라우드의 관점에서 DNS 쿼리는 Wi-Fi 클라이언트가 아닌 Instant AP 클러스터에서 제공되는 것처럼 보일 수 있습니다.

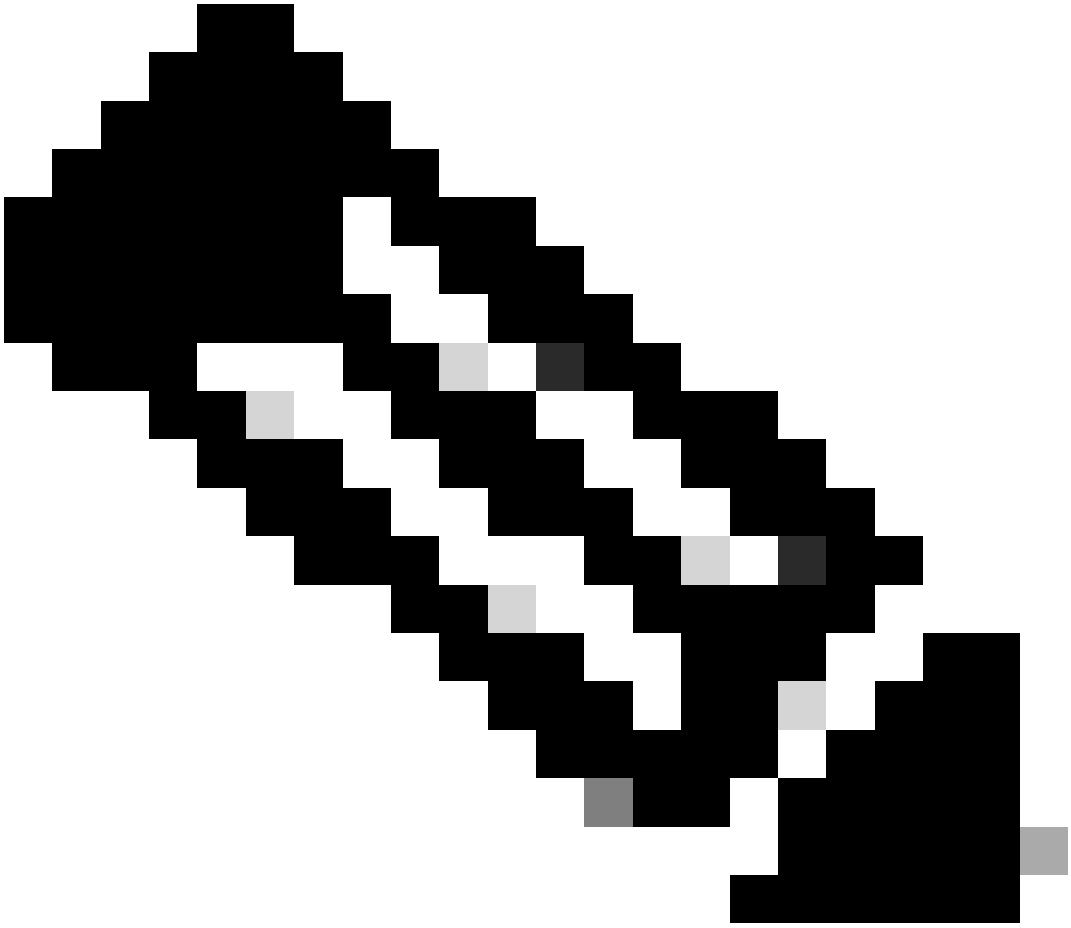
따라서 개별 클라이언트의 DNS 쿼리를 추적하거나 WLAN의 개별 클라이언트에 대한 DNS 정책을 맞춤화해야 하는 경우, Umbrella DNS 사용 설명서에 설명된 표준 방법을 통해(Aruba Instant를 통한 네트워크 디바이스 통합을 사용하지 않고) Umbrella를 구축하고 Umbrella 가상 어플라이언스를 구축 계획에 포함시킬 수 있습니다.

Element	Description
AD User	Identified by Virtual Appliance (VA) or Roaming Client (RC).
AD Computer	Identified by VA only.
Internal Network / Umbrella Site	Identified by VA only.
Default Umbrella Site	Traffic on VA with no other identity. Identified by VA only.
Roaming Client	Roaming Client only.
Network	Network Identity based on source IP of the DNS request.

4403300507924

Aruba Instant Integration

Aruba Instant의 OpenDNS(Umbrella) 네트워크 디바이스 통합은 Instant AP 클러스터에 연결된 모든 Wi-Fi 클라이언트가 단일 Umbrella DNS 정책을 적용받으며, Umbrella 보고서에서 개별 클라이언트의 DNS 쿼리를 검토할 필요가 없는 환경에서 유용합니다. 이 섹션에서는 통합을 설정하는 방법에 대해 설명합니다.



참고: 이 통합에서는 Umbrella의 네트워크 디바이스 API의 레거시 버전을 사용합니다. 기존 버전에서는 고객이 Umbrella 대시보드에서 API 토큰을 생성할 필요가 없지만 최신 버전에서는 이를 생성합니다.

Umbrella 레거시 API는 2023-09-01년에 단종되었으며, 그 이후에는 통합에 대한 지원이 더 이상 제공되지 않습니다. 2023-09-01 이후 통합에 문제가 발생하는 경우, 통합을 사용하지 않고 Umbrella를 구축하려면 구축 설명서의 "시작하기" 섹션을 완료하십시오.

통합을 사용하려면 다음 요건을 충족해야 합니다.

- AP는 InstantOS 버전 8.10.0.1 이상을 실행해야 합니다(2022년 5월 기준).
- 통합에 사용되는 Umbrella 대시보드 계정에는 전체 관리자 역할이 있어야 합니다.
- 계정의 전자 메일 주소를 둘 이상의 Umbrella 대시보드와 연결할 수 없습니다. 이메일 주소가 단일 대시보드에만 연결되어 있는지 확실하지 않은 경우 Cisco Umbrella Support에 문의하여 확인할 수 있습니다.
- 계정에 대해 SSO(Single Sign-On) 및 2FA(2단계 인증)를 활성화할 수 없습니다.
- AP와 인터넷 사이에 네트워크 보안 어플라이언스(예: 방화벽)가 있는 경우 어플라이언스는

208.67.220.220, 208.67.222.222, 67.215.92.210 및 146.112.255.152/29(.152 ~ .159)에 대한 필터링되지 않은 비검사 연결을 허용해야 합니다.

설정

상위 레벨에서는 통합을 활성화하는 네 가지 컨피그레이션 단계가 있습니다.

1. AP 클러스터의 이름 설정

2. 계정 자격 증명을 입력합니다

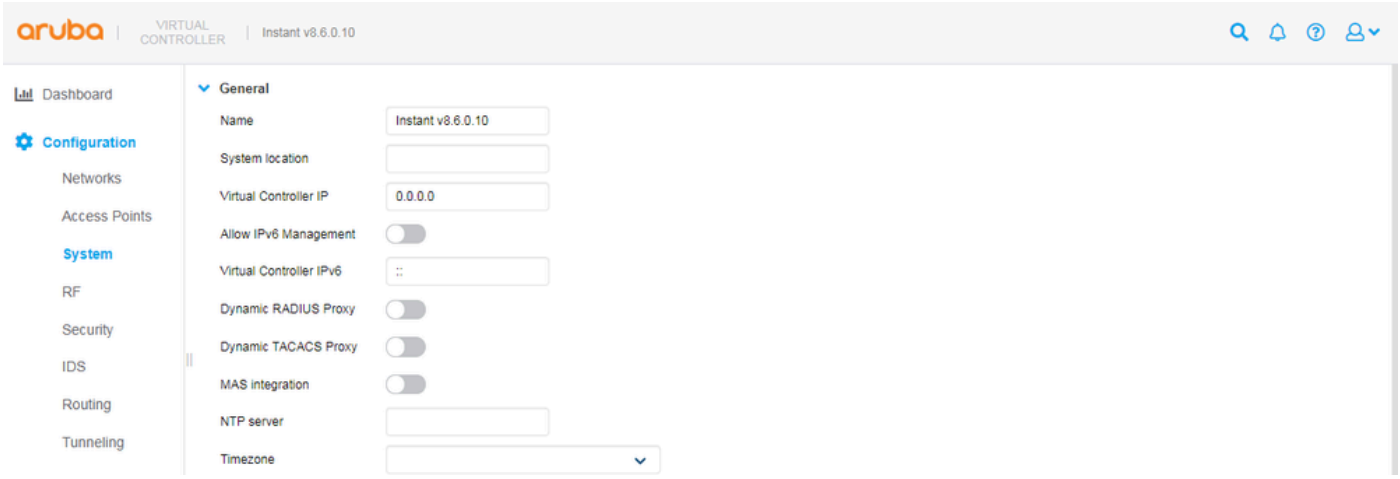
3. DNS 쿼리 가로채기

4. DNS 정책 적용

AP 클러스터의 이름 설정

Instant Cluster가 처음으로 Umbrella 대시보드에 성공적으로 등록되면 Deployments(구축) > Network Devices(네트워크 디바이스) 아래의 Umbrella 대시보드에 네트워크 디바이스 항목이 추가됩니다. 새 항목의 디바이스 이름은 클러스터의 가상 컨트롤러에 구성된 시스템 이름에서 가져옵니다.

Instant Virtual Controller에서 시스템 이름을 설정하려면 Configuration(컨피그레이션) > System(시스템)으로 이동합니다.



4404011628308

이름 값은 초기 등록 과정에서 한 번만 복사됩니다. 나중에 시스템/디바이스 이름이 Instant 또는 Umbrella 측에서 변경된 경우 다른 측에서 이름을 수동으로 업데이트해야 합니다.

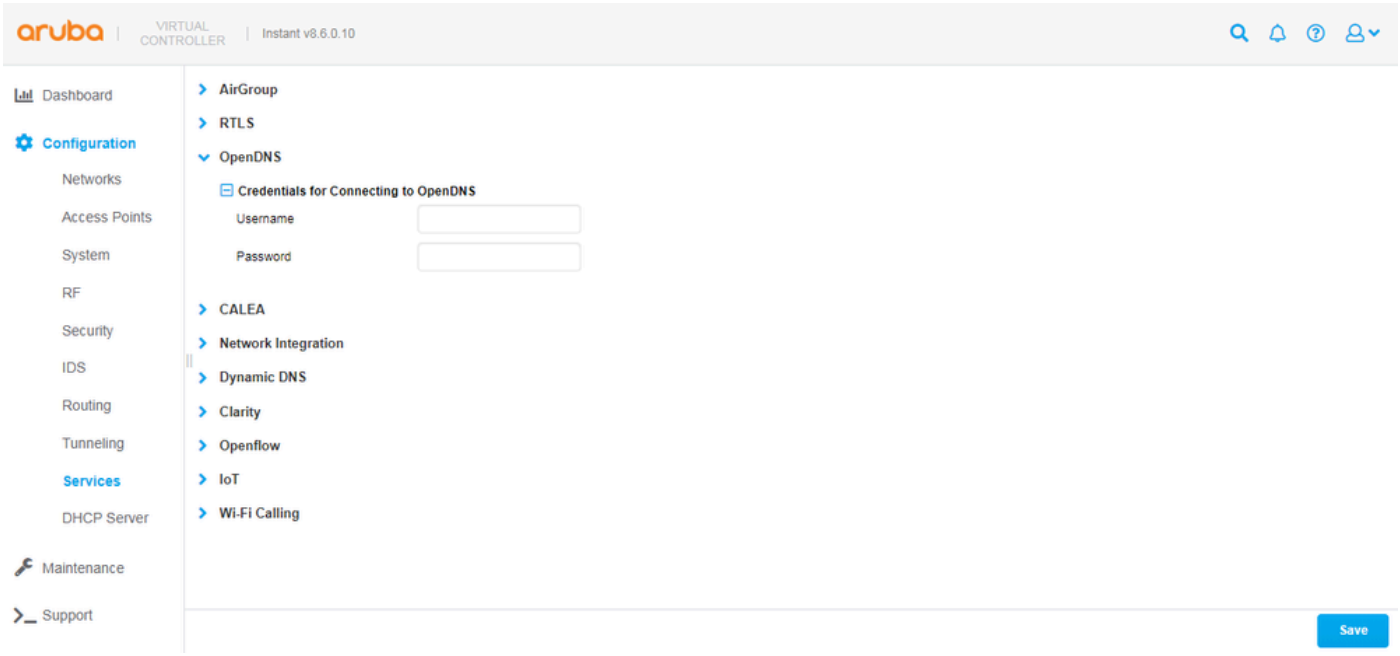
계정 자격 증명 입력

전제 조건 섹션에 나열된 요구 사항이 충족되면 Umbrella 대시보드에 네트워크 디바이스로 Instant 클러스터를 추가할 수 있습니다. 클러스터의 가상 컨트롤러에서 이렇게 하려면

1. Configuration(컨피그레이션) > Services(서비스) > OpenDNS로 이동합니다.

2. Umbrella 계정의 로그인 인증서를 입력합니다.

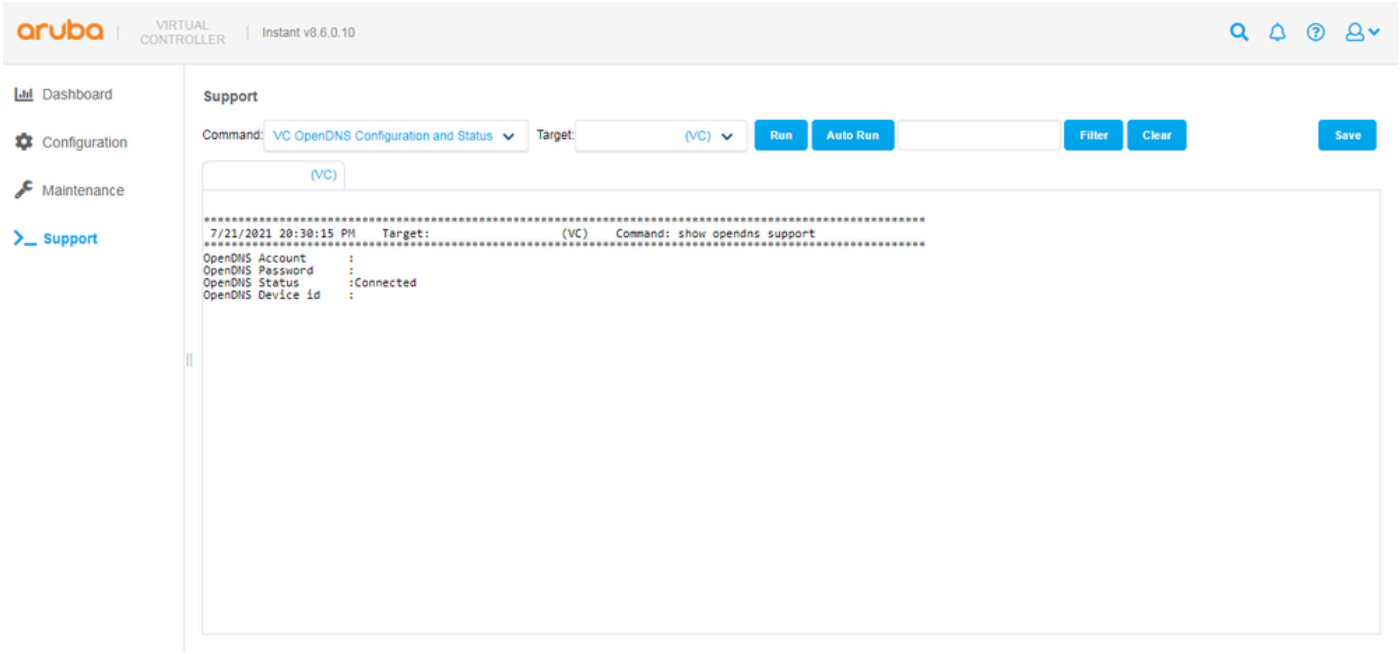
3. 저장을 선택합니다.



4404019266196

VC(가상 컨트롤러)가 Umbrella에 성공적으로 연결되면 Support(지원)로 이동하고 "VC OpenDNS Configuration and Status(VC OpenDNS 컨피그레이션 및 상태)"(`show opendns support`) 명령을 실행할 때 Connected(연결됨) 상태를 볼 수 있습니다.

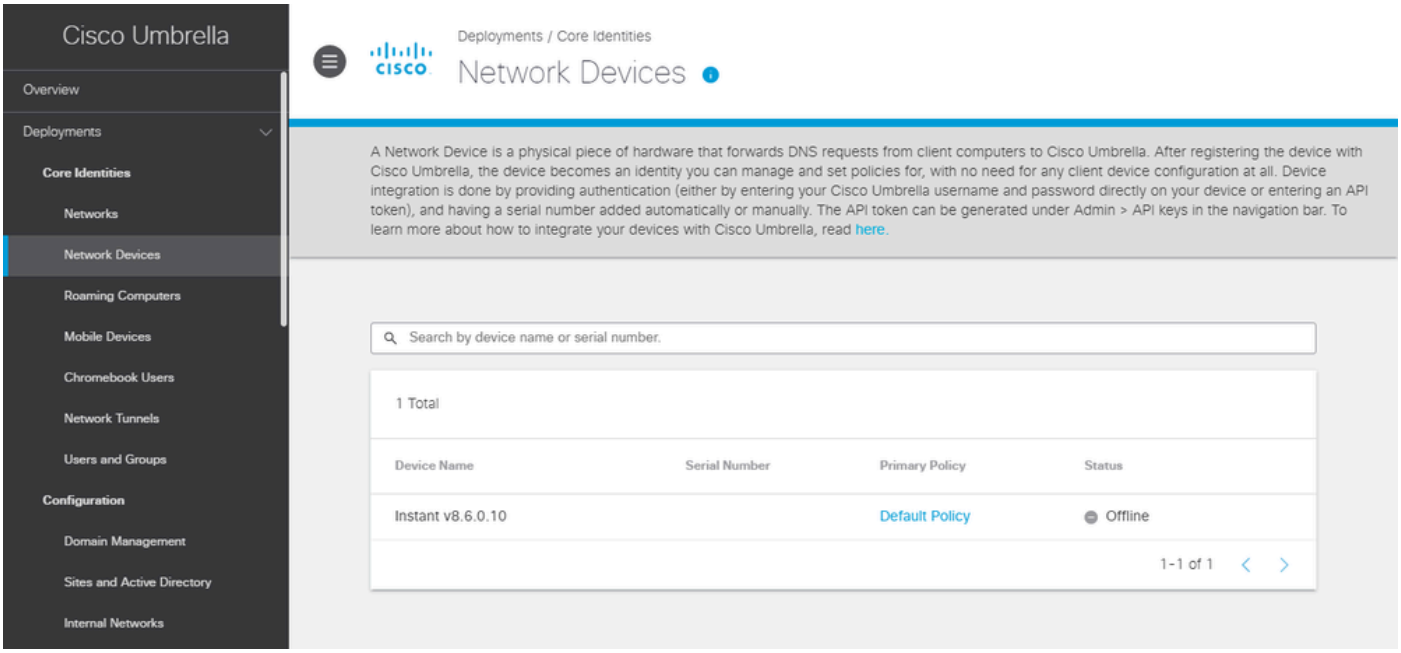
또한 새 네트워크 디바이스가 생성되어 Instant VC 컨피그레이션에 저장될 때 Umbrella에서 생성되는 디바이스 ID를 볼 수 있습니다. 후자가 중요하다. 각 Instant 클러스터에는 고유한 Umbrella 네트워크 디바이스 ID가 있어야 하므로 디바이스 ID를 한 클러스터의 컨피그레이션에서 다른 클러스터로 복사해서는 안 됩니다. 유효한 디바이스 ID는 일반적으로 16자리입니다.



4404019268116

명령 출력에 Not Connected(연결되지 않음) 상태가 표시되면 "AP Tech Support Dump(AP 기술 지원 덤프)"(`show tech-support`) 및 "AP Tech Support Dump Supplemental(AP 기술 지원 덤프 보완)"(`show tech-support supplemental`) 명령을 실행한 다음 로그에서 "opendns"를 검색하면 그 이유를 알 수 있습니다. 문제 해결을 위해 명령 출력을 Aruba TAC와 공유할 수도 있습니다.

모든 것이 올바르게 작동하면 Umbrella 대시보드의 Deployments(구축) > Network Devices(네트워크 디바이스) 아래에 새 항목이 표시됩니다. 이에서 해당 이름으로 Instant AP 클러스터를 검색하거나 새 디바이스 ID를 생성하려는 경우 기존 항목을 삭제할 수 있습니다.



4404011658516

Intercept DNS Queries(가로채기 DNS 쿼리)

클러스터가 Umbrella 대시보드에 네트워크 디바이스로 성공적으로 추가되었음을 확인하면 클러스터의 AP에 연결된 무선 클라이언트에서 보낸 DNS 쿼리를 인터셉트하도록 클러스터를 설정할 수 있습니다. 일단 설정되면 무선 클라이언트의 NIC에 어떤 DNS 서버 IP 주소가 구성되었는지에 관계없이 클라이언트의 DNS 쿼리는 클러스터에서 가로채서 208.67.220.220 및 208.67.222.222의 Umbrella의 애니캐스트 리졸버로 전달될 수 있습니다.

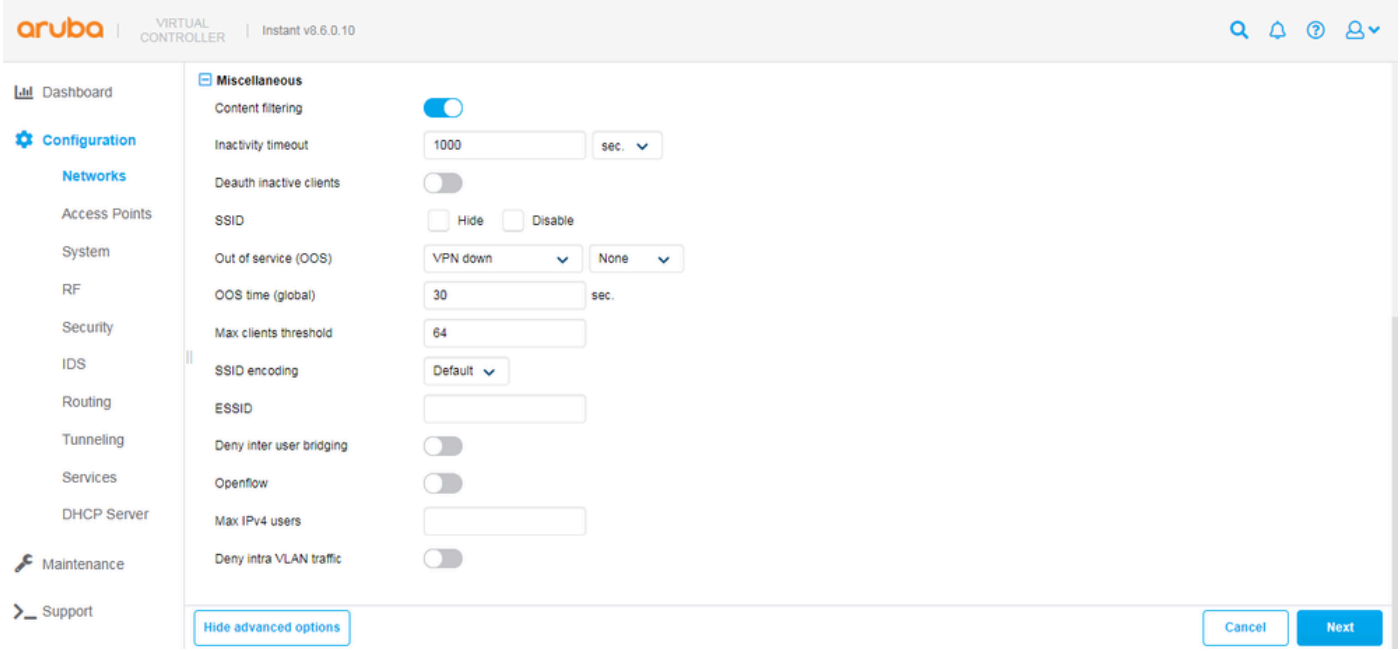
DNS 쿼리를 가로채려면

1. Configuration(컨피그레이션) > Networks(네트워크)에서 클러스터의 가상 컨트롤러로 이동합니다.

2. 무선 네트워크를 선택합니다.

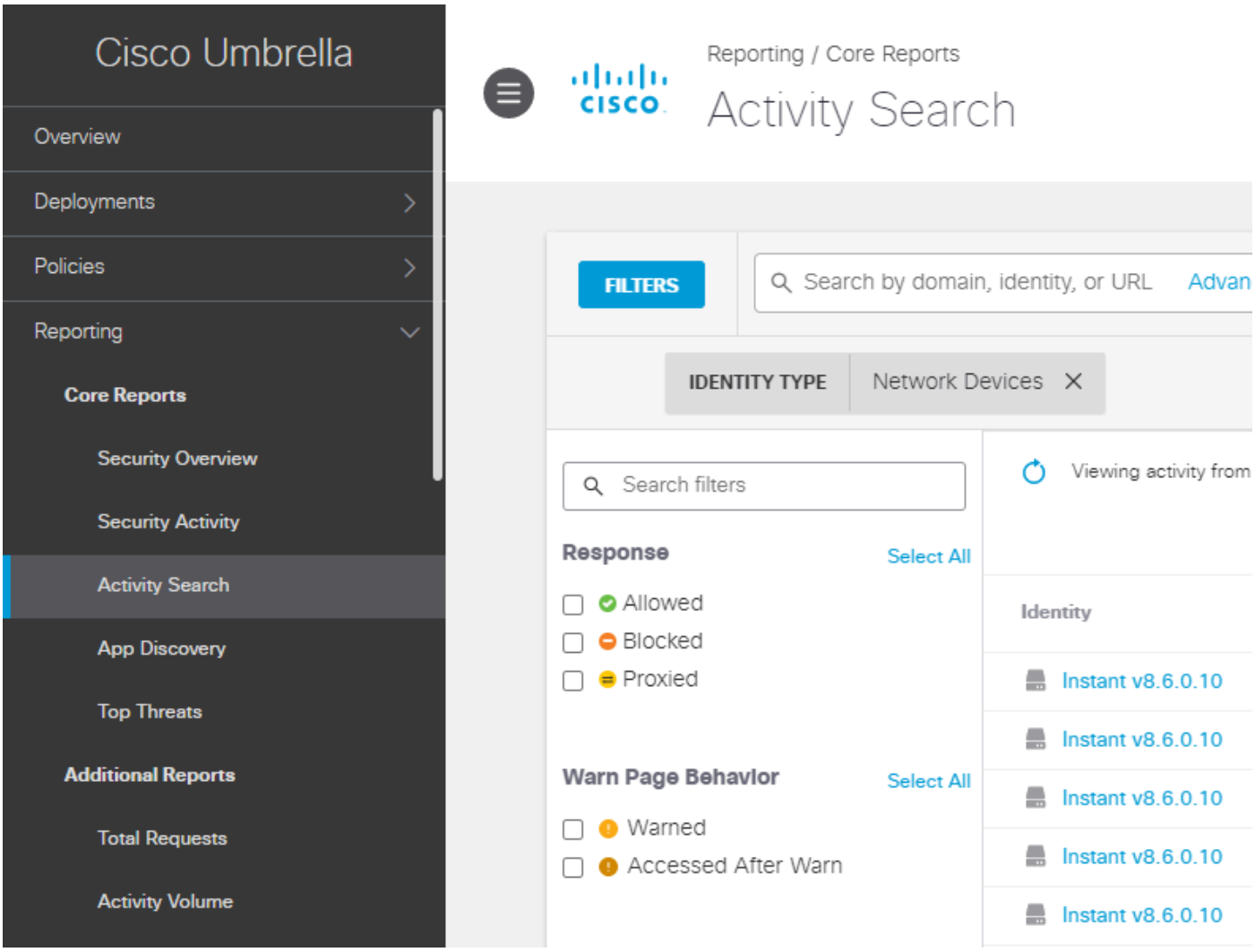
3. 네트워크를 편집하고, 고급 옵션 표시를 선택한 후, 기타 섹션으로 스크롤합니다.

4. 콘텐츠 필터링 옵션을 활성화하고, 완료 버튼을 선택하여 변경 사항을 저장할 수 있을 때까지 다음 선택을 유지합니다.



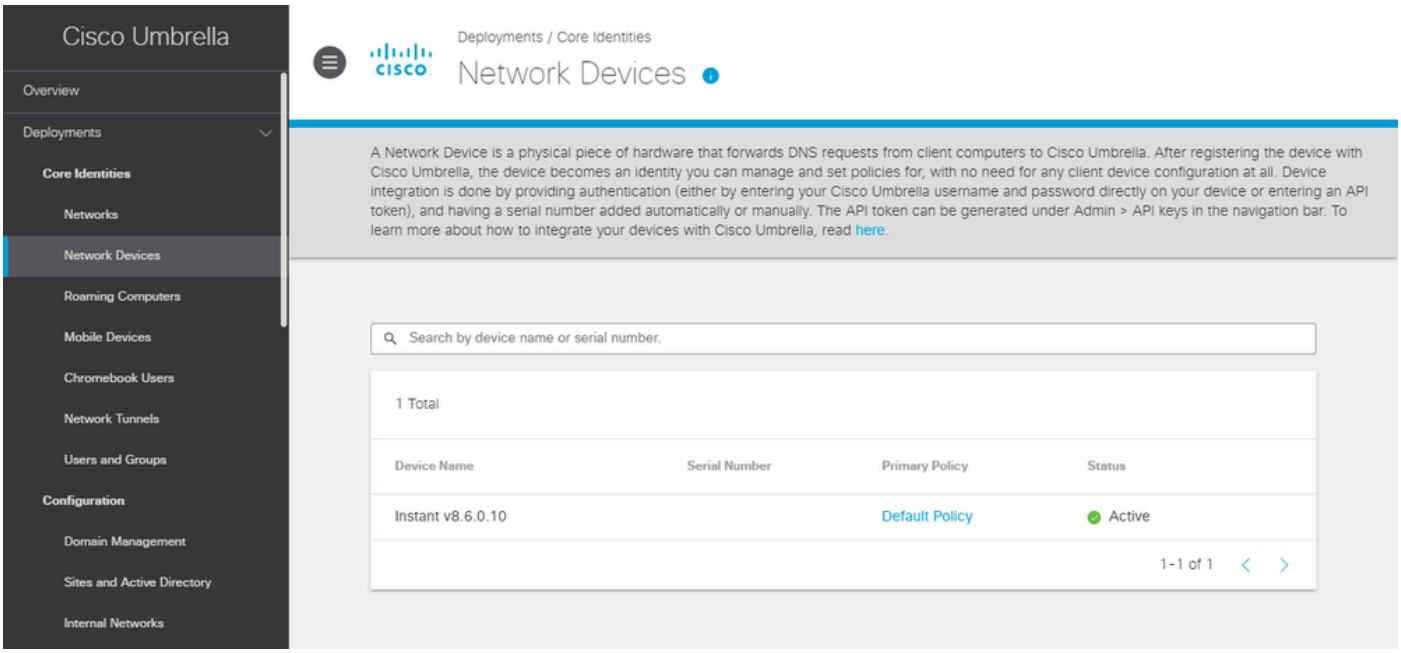
4404011668500

이 옵션을 설정한 후 Umbrella 대시보드의 Reporting(보고) > Activity Search(활동 검색)에서 DNS 쿼리를 볼 수 있습니다.쿼리의 ID는 일반적으로 AP 클러스터의 가상 컨트롤러에 구성된 시스템 이름인 네트워크 디바이스 이름에 매핑될 수 있습니다. 쿼리를 처리하고 대시보드 GUI에 표시하는 데 다소 시간(약 15분)이 걸릴 수 있습니다.



4404011721620

Deployments(구축) > Network Devices(네트워크 디바이스) 아래의 Umbrella 대시보드에서 디바이스가 활성/온라인 상태로 변경되는 데 최대 24시간이 걸릴 수 있습니다. 네트워크 디바이스의 상태는 24시간 전에 디바이스에서 DNS 쿼리를 가로채서 Umbrella로 전달했는지 여부만 나타낼 뿐 디바이스가 Umbrella와 통신하는 방식에는 영향을 주지 않습니다. 오프라인/비활성 상태는 지난 24시간 동안 무선 클라이언트가 AP 클러스터에 연결되지 않았음을 의미할 수 있으며, 클러스터가 Umbrella 서비스를 사용하는 것을 막을 수 없습니다.

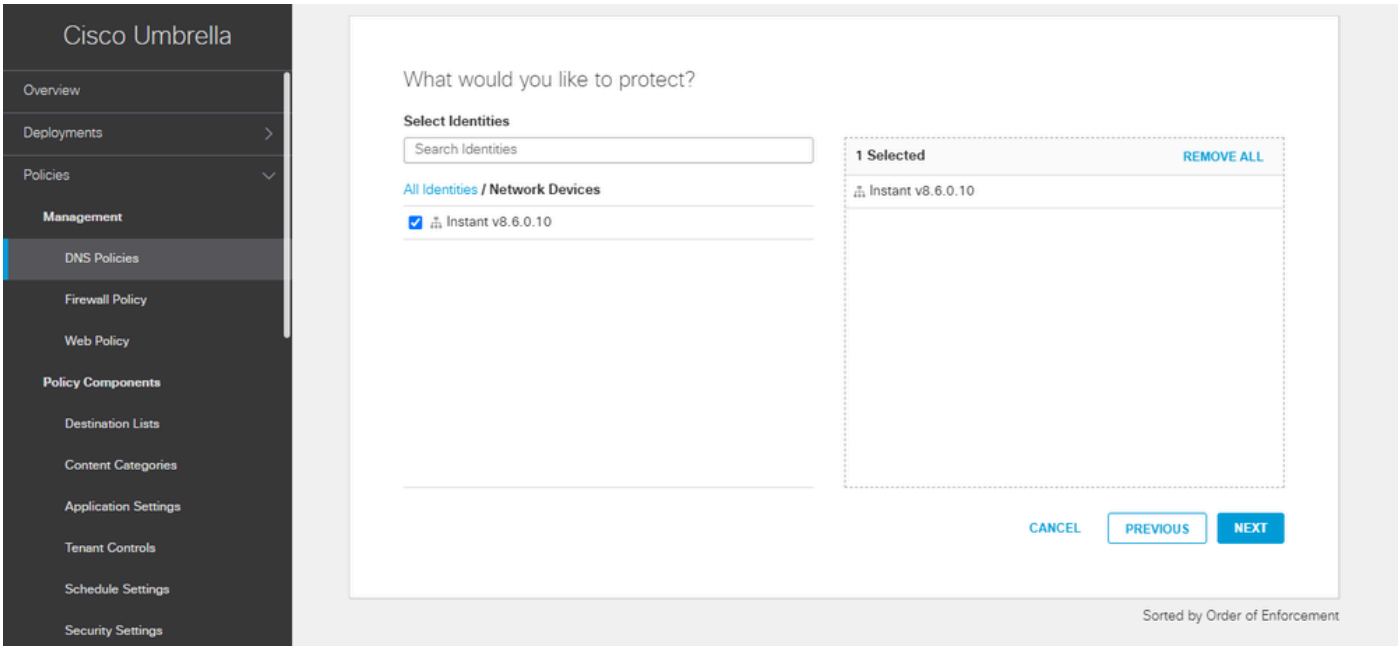


4404011756308

DNS 정책 적용

Umbrella에서 "기본 정책"은 대시보드에 추가된 모든 ID(예: 네트워크 디바이스)를 자동으로 포함합니다. 구축의 모든 AP 클러스터가 동일한 정책의 적용을 받을 수 있는 경우 추가 DNS 정책을 생성할 필요가 없습니다. 이 경우 다음 섹션으로 건너뜁니다.

또는 특정 네트워크 디바이스에 사용자 지정 정책을 적용하려면 Umbrella 대시보드의 Policies(정책) > All Policies(모든 정책)(DNS Policies(DNS 정책))에서 새 정책을 추가하고 정책에서 네트워크 디바이스를 선택해야 합니다.



4404011773588

DNS Policies (All Policies)(DNS 정책(모든 정책)) 페이지에 둘 이상의 정책이 있는 경우, 정책은 첫 번째 일치 기준으로 위에서 아래로 평가됩니다. 자세한 내용은 정책 우선 순위 설명서 및 정책 설명

서 정의 모범 사례를 참조하십시오.

내부 DNS

내부 DNS 서버가 있고 특정(내부) 도메인에 대한 DNS 쿼리를 내부 DNS 서버로 전달하려는 환경에서는 Instant에서 Enterprise Domains 기능을 사용할 수 있습니다.

DNS 쿼리는 이 기능이 활성화된 후에도 AP 클러스터에서 계속 인터셉트될 수 있습니다. 단, 지정된 도메인에 대한 쿼리는 더 이상 Umbrella로 전달될 수 없습니다. 대신, 무선 클라이언트의 NIC에 원래 구성된 DNS 서버 IP 주소로 (DHCP를 통해) 전달될 수 있습니다. 이 기능은 Aruba Instant Integration이 사용되지 않는 표준 Umbrella 구축 방법(가상 어플라이언스 포함)에서 사용할 수 있는 Internal Domains 기능과 유사합니다.

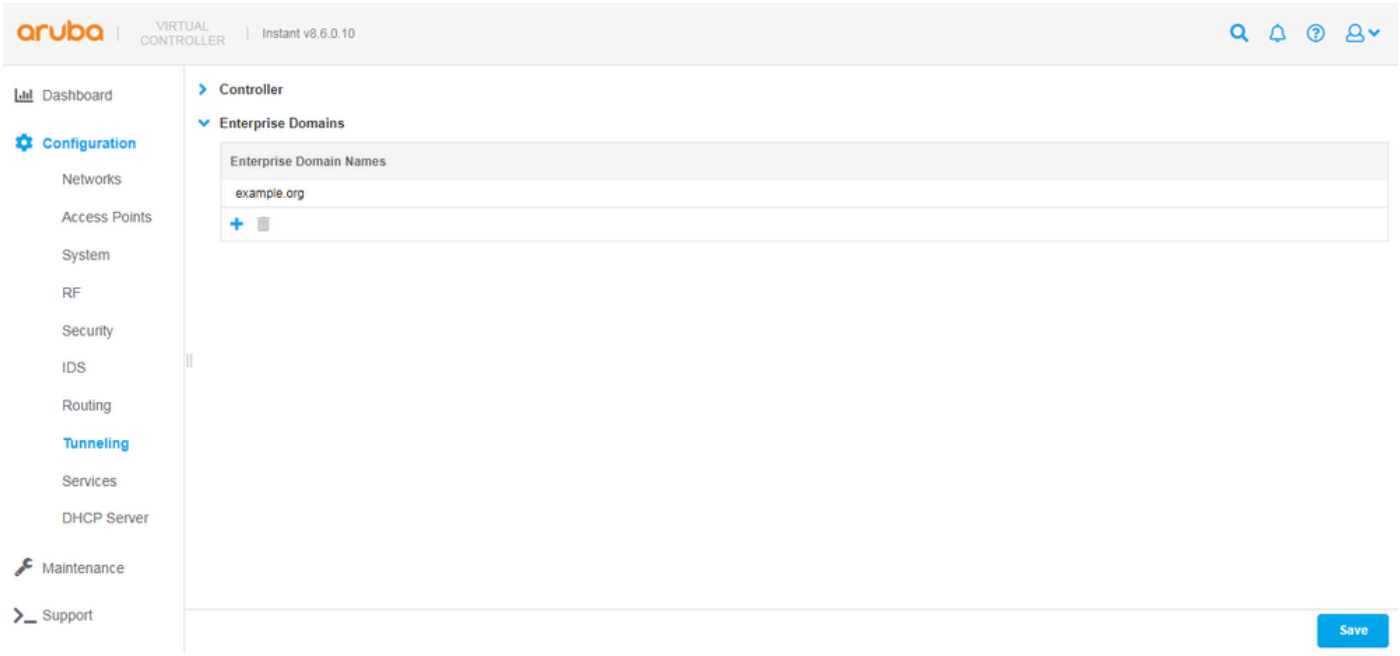
Instant Virtual Controller에서 기능을 구성하려면

1. Configuration(구성) > Tunneling(터널링) > Enterprise Domains(엔터프라이즈 도메인)로 이동합니다.

2. 엔터프라이즈 도메인 이름 목록에 도메인을 추가하거나 제거합니다.

3. 저장을 선택합니다.

목록에 추가된 모든 도메인에 대해 암시적 와일드카드가 있으므로 example.org은 *.example.org을 의미합니다.

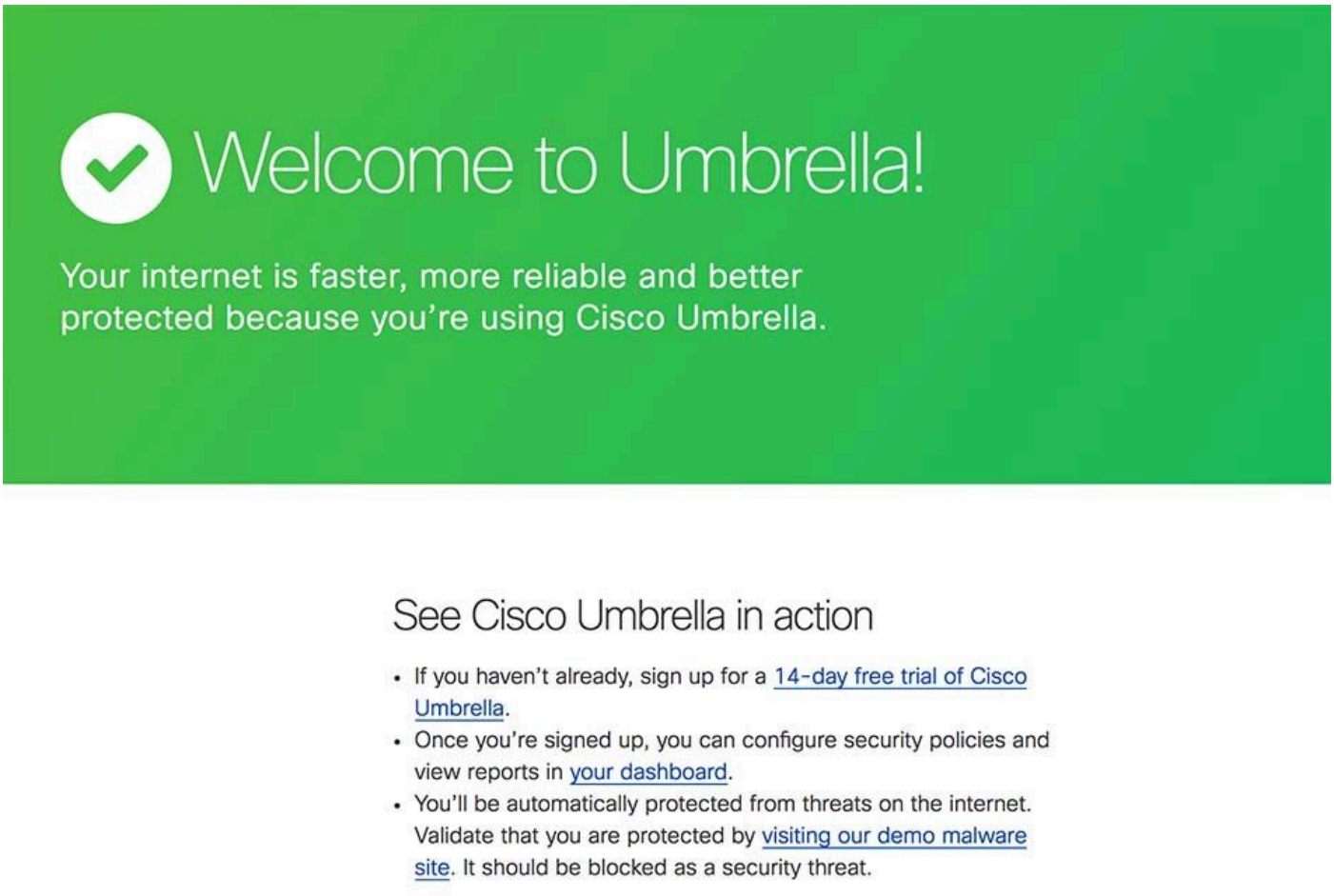


4404238114452

확인

이 설명서의 "구축 개요" 섹션에서 참조하는 표준 방법을 사용하여 WLAN에 Umbrella를 구축했는지 또는 "Aruba Instant Integration" 섹션에서 설명하는 통합을 사용했는지 여부와 상관없이, 클라이언트 중 하나에서 https://welcome.umbrella.com/으로 이동하여 무선 클라이언트가 Umbrella

DNS를 사용하고 있는지 확인할 수 있습니다. 그런 다음 Umbrella 문서에 표시된 스크린샷과 유사한 녹색 확인 표시가 나타납니다.



4404011960212

또는 무선 클라이언트의 명령 프롬프트에서 이 명령을 실행하여 이를 확인할 수 있습니다.

```
nslookup -type=txt debug.opendns.com.
```

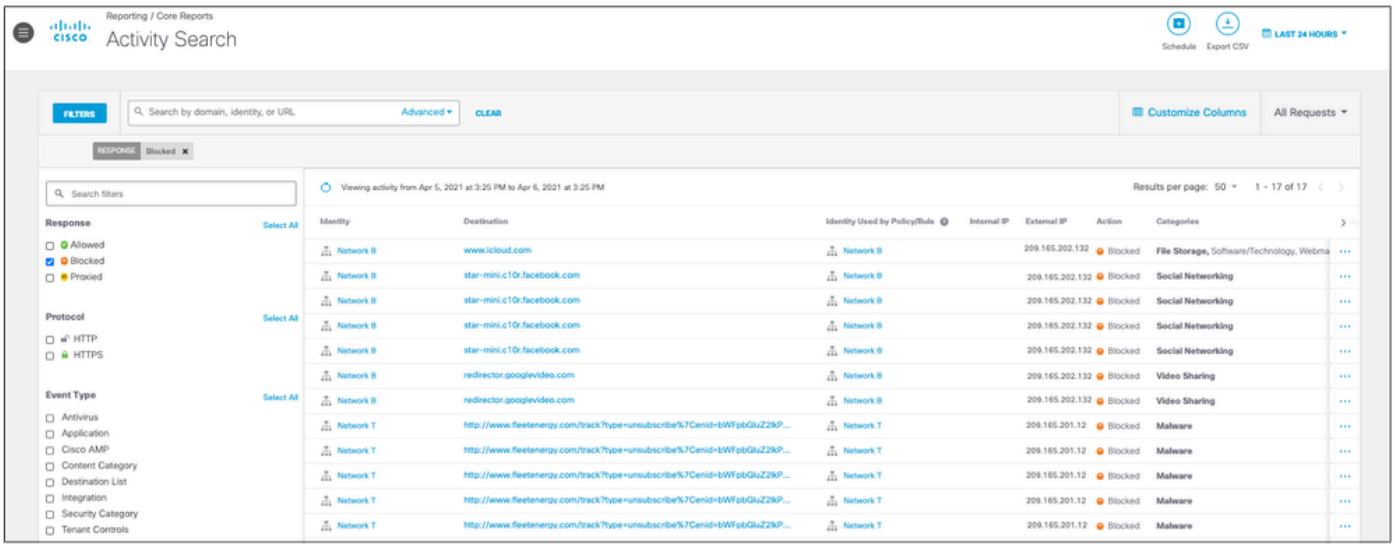
이 스크린샷과 유사한 여러 개의 텍스트 줄이 있는 출력을 볼 수 있습니다.

```
anthony@ubuntu:~/Desktop$ nslookup -type=txt debug.opendns.com.
Server:         127.0.1.1
Address:        127.0.1.1#53

Non-authoritative answer:
debug.opendns.com       text = "server 7.pao"
debug.opendns.com       text = "organization id
debug.opendns.com       text = "appliance id
debug.opendns.com       text = "host id
debug.opendns.com       text = "user id
debug.opendns.com       text = "remoteip
debug.opendns.com       text = "flags
debug.opendns.com       text = "id
debug.opendns.com       text = "source
debug.opendns.com       text = "fw: flags
debug.opendns.com       text = "fw: id
debug.opendns.com       text = "fw: source

Authoritative answers can be found from:

anthony@ubuntu:~/Desktop$
```

4404011980436

명령 출력에서 "orgid" 또는 "organization id" 줄에 Umbrella 대시보드의 org ID를 볼 수 있으며 Instant Integration을 사용하는 경우 디바이스 ID가 포함된 추가 "device" 줄을 볼 수 있습니다.

Umbrella 대시보드에서 DNS 쿼리를 검토하려면 Reporting(보고) > Activity Search(활동 검색)로 이동합니다. 쿼리가 대시보드 GUI에 표시되는 데에는 약간의 시간(약 15분)이 걸릴 수 있습니다. 활동 검색 사용 방법에 대한 지침은 Umbrella 문서에서 확인할 수 있습니다.



4404019393044

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.